

19 marca w Sejmie odbyło się posiedzenie Podkomisji stałej ds. młodzieży. W trakcie spotkania poruszono zagadnienia cyberbezpieczeństwa w szkołach i placówkach oświatowych, a także zwrócono uwagę na ogólny problem dużej ilości szkodliwych i niebezpiecznych treści, do których dzieci i młodzież mają łatwy dostęp.

Umiejętności cyfrowe to podstawa

Posiedzenie rozpoczęło się od wypowiedzi dyrektora ds. Ogólnopolskiej Sieci Edukacyjnej Przemysława Kuny. Zabierając głos na temat problematyki cyberbezpieczeństwa i strategii jego poprawy, odniósł się do dokumentu pt. "Polityka Cyfrowej Transformacji Edukacji" przyjętego we wrześniu 2024 r. Cyberbezpieczeństwo jest w tej koncepcji jednym z wyszczególnionych tematów, zaś cele mające służyć jego zwiększeniu, zostały rozpisane wraz z planem wdrażania do 2035 roku. Dyrektor Kuna zwrócił w tym kontekście uwagę na szczególną rolę tzw. kompetencji cyfrowych, które w opracowanym przez Instytut Badań Edukacyjnych profilu absolwenta zostały umieszczone wśród umiejętności fundamentalnych. Rozwój tych umiejętności ma odbywać się na polu dużo szerszym niż obecnie, bowiem ich uwzględnianie będzie miało miejsce nie tylko na informatyce, lecz również w przedmiotach pozornie mniej związanych z tematem, chociażby przedmiotach humanistycznych. Duży nacisk kładzie się także na rozwój kompetencji cyfrowych nauczycieli, dla których przewidziane zostaną szkolenia na dużą skalę, uzupełniające te regionalne czy organizowane na poziomie szkół. Już w tym roku odbędzie się duże szkolenie poświęcone szansom i zagrożeniom, jakie niesie sztuczna inteligencja. Oprócz szkoleń ogólnych i służących podnoszeniu poziomu tam, gdzie aktualnie jest jeszcze zbyt niski, przedstawiona zostanie oferta szkoleń na poziomie zaawansowanym, wśród których kluczowym tematem będzie właśnie cyberbezpieczeństwo. Jako że w pojęciu tym zawiera się szereg niezbędnych umiejętności związanych z korzystaniem z narzędzi cyfrowych, opracowywane są materiały, broszury, poradniki i scenariusze zajęć zwiększające wiedzę z tego zakresu.

Ochrona szkolnych sieci na wielu płaszczyznach

Kolejno, głos zabrała zastępczyni dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji Monika Pieniek. Przechodząc do działań podejmowanych w celu poprawy bezpieczeństwa cyfrowego szkół i placówek oświatowych, powołała się na najnowsze dane dotyczące problematyki zagrożeń cyfrowych. Jak wynika z badań, w 2024 roku w środowisku oświaty i wychowania zarejestrowano 714 incydentów, stanowiących ok. 0,9% wszystkich, jakie wystąpiły i zostały zgłoszone. Dotyczyły szkół każdego rodzaju, a także bibliotek i uczelni wyższych. Jak wskazano, wzrost liczby takich incydentów w porównaniu z rokiem 2023 nie świadczy jeszcze o nowym, poważnym kryzysie. Ilość przypadków znanych odpowiednim instytucjom wynika bowiem także ze wzrostu świadomości społecznej dotyczącej konieczności zgłaszania tego typu incydentów. W celu ich zapobiegania, wprowadzono Ogólnopolską Sieć Edukacyjną, która gwarantuje szkołom w całej Polsce dostęp do szybkiego i bezpiecznego internetu. Do programu przystąpiło już 90,5% wszystkich szkół, co sprzyja wyrównywaniu szans na realizowanie obowiązków dotyczących cyberbezpieczeństwa. W ramach Sieci świadczona jest usługa "bezpieczny internet", chroniąca przed treściami potencjalnie szkodliwymi, a także przeciwdziałająca atakom i instalowaniu wirusów. Przewidziany został dostęp standardowy, a także dodatkowo płatny dostęp o zwiększonej przepustowości, ponadto pakiet zaawansowanych usług chroniących dodatkowo przed szkodliwym oprogramowaniem. Elementy sieci są monitorowane całodobowo, dzięki czemu w minionym roku udało się udaremnić ponad 700 ataków DDoS. Jak przekazała Monika Pieniek, w ramach OSE realizowane są także inne działania wspierające edukację, w tym dwa e-learningi (IT szkoła i Bezpieczni w sieci). Dostępne są również webinary i spotkania

poświęcone tematyce, adresowane aktualnym i potencjalnym uczestnikom, a także bezpłatna aplikacja mOchrona służąca ochronie przed niebezpiecznymi treściami. Szczególną uwagę zwraca się również na dostępne od 2021 roku tzw. cyberlekcje - projekt wspierający nauczanie o cyberbezpieczeństwie. Odnotowano potrzebę wsparcia nauczycieli w wykorzystywaniu narzędzi, które już są dostępne. Realizowane są szkolenia, zaś scenariusze cyberlekcji są na bieżąco rewidowane. Pobrano je już 12 tys. razy.

Walka z niebezpieczeństwami może być trudna

Kolejno, głos zabrali parlamentarzyści, którzy oprócz zadawania pytań, zwrócili uwagę także na inne naglące problemy. Posłanka PiS Dominika Chorościńska wyraziła zaniepokojenie związane z bardzo dużą skalą niebezpiecznych zachowań i treści, których wg. najnowszego raportu NASK doświadczają dzieci. Zdecydowana większość niebezpieczeństw czyha poza szkołą, stąd zgłoszona została potrzeba głębszego zastanowienia się nad tym, w jaki sposób można chronić najmłodszych przed zagrożeniami, z jakimi spotykają się chociażby w domowym zaciszu. Poseł KO Adam Krzemiński zwrócił z kolei uwagę na potrzebę przeprowadzenia akcji informacyjnych kierowanych do rodziców, którzy często nie rozumieją natury najpoważniejszych obecnie zagrożeń z zakresu cyberbezpieczeństwa. Podobne przekonanie wyraził poseł Lucjan Pietrzych, którego zdaniem niejednokrotnie nauczyciele mają opory przed zwróceniem uwagi rodzicom uczniów, gdyż tamci mają bardzo wysokie mniemanie o swojej wiedzy i stosowanych metodach wychowawczych. Poseł Marcin Józefaciuk podniósł potrzebę zaangażowania w prowadzone prace większej ilości podmiotów, w celu realizowania polityki cyfrowej w sposób pełny i gwarantujący efektywność. Bezpieczna powinna być bowiem cała administracja placówek oświatowych, nie wyłączając ośrodków wychowawczych, terapeutycznych i bibliotek. Poseł Józefaciuk wskazał, że dyrektorzy placówek potrzebują przede wszystkim realnych narzędzi teleinformatycznych, a nie tylko procedur odkładanych później na przysłowiową półkę. Poseł Sławomir Skwarek zauważył ponadto potrzebę wdrożenia zmian legislacyjnych, które zagwarantowałyby zachowanie odpowiednich standardów cyberbezpieczeństwa.

W odpowiedzi na zadane pytania i wyrażone wątpliwości, dyr. Przemysław Kuna wskazał na obowiązek odpowiedniego zabezpieczenia dostępu do szkolnego internetu, który istnieje już obecnie. Konieczne będzie natomiast wypracowanie procedur dotyczących zgłaszania incydentów, a także samodoskonalenia nauczycieli, których szkolenia nie są w stanie zastąpić z uwagi na dynamicznie zmieniającą się sytuację i zagrożenia niesione przez szybki postęp technologiczny. Dyrektor zwrócił uwagę na trudności, z jakimi wiąże się zaangażowanie rodziców niejednokrotnie zasłaniających się brakiem czasu i niechętnych do współpracy w obszarze poprawy bezpieczeństwa młodych osób w sieci.

Mając na uwadze obszerność tematu cyberbezpieczeństwa, uczestnicy posiedzenia zgodzili się co do potrzeby kontynuowania rozmów. Kolejne posiedzenie podkomisji zostanie najprawdopodobniej poświęcone skuteczności wdrażanych rozwiązań.

Źródło: iTV Sejm